




IDENTITY MANAGER INTEGRATION WITH ARUBA

SECTION C

WHAT YOU WILL LEARN

- > Run the wizard to setup a guest network
- > Add IDM as the RADIUS Server
- > Set IDM as the external web portal
- > Configure IDM for the Aruba Controller

LOGIN TO THE WEB CONSOLE



The image shows a screenshot of the Aruba Networks login web console. The background is a dark gray rectangle. In the center is a white rectangular area containing the login form. At the top of the white area is the Aruba Networks logo, with 'ARUBA' in orange and 'networks' in gray. Below the logo is the text 'Please Login' in bold black. Underneath is a 'User:' label followed by a text input field with a blue border. Below that is a 'Password:' label followed by a text input field. A 'Login' button is centered below the password field. At the bottom of the white area, the text 'System Name : Aruba620' is displayed.

ARUBA
networks

Please Login

User:

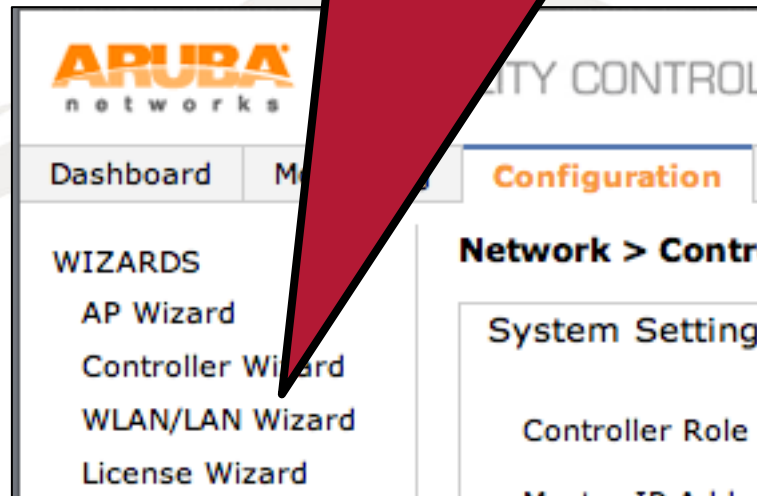
Password:

Login

System Name : Aruba620

START THE WLAN WIZARD

1. Configuration > WLAN/LAN Wizard



CHOOSE THE DEPLOYMENT SCENARIO

1. Select Campus Only

ARUBA networks MOILITY

Dashboard Monitoring **Configure** Diagnostics Maintenance Plan

Save Configuration Logout admin

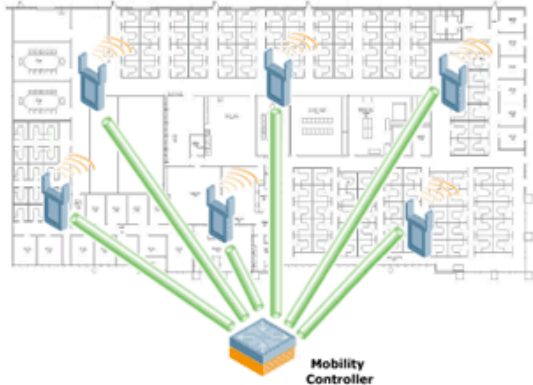
Configure WLAN/LAN

Welcome to the WLAN/LAN Configuration Wizard

Deployment scenario:

- ☒ Campus Only -- all of the access points will be physically connected to the local controller
- ☐ Remote Networking -- some of the access points will be deployed at remote locations

Campus Wireless



Mobility Controller

2. Click Begin

Begin Cancel

SELECT THE AP GROUP

The screenshot shows the Aruba Mobility Controller configuration page for 'Configure WLAN/LANs'. The interface includes a top navigation bar with tabs for Dashboard, Monitoring, Configuration (selected), Diagnostics, Maintenance, and Plan. A 'Save Configuration' button and a 'Logout admin' link are also present. The main content area is divided into two sections: '1 Group' and '2 Wireless LANs'. The '1 Group' section is active, showing a 'Specify Group to Configure' form. This form includes a text description of AP groups, a 'Group' dropdown menu currently set to 'default', and a 'New' button. A 'Workflow' sidebar on the left shows steps 1 and 2, with step 1 'Group to Configure' highlighted in green. A red callout bubble labeled '1. Select default' points to the 'default' option in the dropdown menu. At the bottom right of the form, there are 'Next' and 'Cancel' buttons. A second red callout bubble labeled '2. Click Next' points to the 'Next' button.

ARUBA networks MOILITY CONTROLLER

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

Configure WLAN/LANs

1 Group **2 Wireless LANs**

Workflow Help

1 Group to Configure

Specify Group to Configure

An AP group is a set of APs that share Wireless LAN parameters. Initially there is a single group named Default. If you wish, you can create multiple groups. [More...](#)

Group New

Note: The setting you select in the Wireless LAN will apply to the Group you select here. If you configure multiple groups you can make multiple passes through Wizards.

Next Cancel

CREATE THE GUEST WLAN

ARUBA networks MOBIILITY CONTROLLER | Aruba620

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

Configure WLAN/LANs

1 Group **2 WLAN**

Workflow Help

1 WLAN

2 Forwarding Mode

3 Radio & VLAN

4 Internal/Guest

5 Authentication and Encryption

6 Captive Portal

7 Authentication Server

8 Roles & Policies

9 Role Assignment

10 WLAN Configured

Specify Wireless LAN (WLAN) for Group default

APs are organized into AP groups, and each AP group can have one or more WLANs. You can edit an existing WLAN or create a new WLAN. If you choose to edit an existing WLAN, note that WLANs can be assigned to multiple AP groups. Edit the shared WLAN if you wish to affect all AP groups, or edit a copy of the WLAN if you wish to affect only the selected AP group. [More...](#)

AP Groups	All WLANs	Sharing
default		

New Copy Delete

Create new WLAN named:

OK Cancel

You can:

- ➔ Select an existing WLAN in the table and clicking **New**
- ➔ Create a new WLAN by selecting any Group and clicking **Copy**
- ➔ Create a new WLAN by selecting any Group and clicking **Share**
- ➔ Share a new WLAN that belongs to another Group by selecting the WLAN and clicking **Share**

Back Next Cancel

SPECIFY THE FORWARDING MODE

The screenshot displays the Aruba Mobility Controller configuration page for 'Aruba620'. The 'Configuration' tab is active, and the 'Configure WLAN/LANs' section is selected. The left sidebar shows a workflow with 10 steps: 1. WLAN, 2. Forwarding Mode, 3. Radio & VLAN, 4. Internal/Guest, 5. Authentication and Encryption, 6. Captive Portal, 7. Authentication Server, 8. Roles & Policies, 9. Role Assignment, and 10. WLAN Configured. The main content area is titled 'Specify Forwarding Mode for aruba-guest-network in Group default'. It explains that the Forwarding Mode provides options for forwarding traffic back to the controller through the IPsec tunnel. The 'Forward Mode' section has three radio buttons: 'Tunnel' (selected), 'Decrypt-Tunnel', and 'Bridge'. A red callout box labeled '1. Select Tunnel' points to the 'Tunnel' radio button. Below the radio buttons, a text box states: 'In Tunnel mode, the traffic is forwarded back to the controller through the IPsec tunnel.' At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'. A red callout box labeled '2. Click Next' points to the 'Next' button.

ARUBA networks MOBILITY CONTROLLER | Aruba620

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Config

Configure WLAN/LANs

1 Group **2 Wireless LAN**

Workflow Help

1 WLAN
APGroup: default
SSID: aruba-guest-network

2 Forwarding Mode

3 Radio & VLAN

4 Internal/Guest

5 Authentication and Encryption

6 Captive Portal

7 Authentication Server

8 Roles & Policies

9 Role Assignment

10 WLAN Configured

Specify Forwarding Mode for aruba-guest-network in Group default

The Forwarding Mode provides a range of options for forwarding traffic back to the controller through the IPsec tunnel. [More...](#)

Forward Mode:

☒ Tunnel In Tunnel mode, the traffic is forwarded back to the controller through the IPsec tunnel.

☐ Decrypt-Tunnel

☐ Bridge

Back Next Cancel

SPECIFY THE RADIOS AND VLAN

The screenshot shows the Aruba Mobility Controller configuration page for 'Aruba620'. The 'Configuration' tab is active. The left sidebar shows a workflow with 10 steps: 1. WLAN, 2. Forwarding Mode, 3. Radio & VLAN, 4. Internal/Guest, 5. Authentication and Encryption, 6. Captive Portal, 7. Authentication Server, 8. Roles & Policies, 9. Role Assignment, and 10. WLAN Configured. Step 3 is highlighted. The main content area is titled 'Specify Radio Type and VLAN for aruba-guest-network in Group default'. It contains a 'Radio Type' dropdown set to 'all' and a 'VLAN' field set to '1'. A red arrow points from the '1. Specify VLAN' callout to the 'VLAN' field. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons. A red arrow points from the '2. Click Next' callout to the 'Next' button.

ARUBA networks MOILITY CONTROLLER | Aruba620

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration

Configure WLAN/LANs

1 Group **2 Wireless LANs**

Workflow ? Help

1 WLAN
APGroup: default
SSID: aruba-guest-network

2 Forwarding Mode
Tunnel

3 Radio & VLAN

4 Internal/Guest

5 Authentication and Encryption

6 Captive Portal

7 Authentication Server

8 Roles & Policies

9 Role Assignment

10 WLAN Configured

Specify Radio Type and VLAN for aruba-guest-network in Group default

Specify the radio type on which this SSID is available, as well as the VLAN in which users connecting to this SSID are to be placed by default. Note: you can override the VLAN specified below by configuring per-role VLANs in Step 8. [More...](#)

Radio Type: all

VLAN: 1 <-- 1

Back Next Cancel

SPECIFY THE WLAN IS FOR GUESTS

ARUBA networks MOILITY CONTROLLER | Aruba620

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Plan | Save Configuration

Configure WLAN/LANs

1 Group **2 Wireless LANs**

Workflow ? Help

- 1 WLAN**
APGroup: default
SSID: aruba-guest-network
- 2 Forwarding Mode**
Tunnel
- 3 Radio & VLAN**
Radio Type: all
VLAN: 1
- 4 Internal/Guest**
- 5 Authentication and Encryption
- 6 Captive Portal
- 7 Authentication Server
- 8 Roles & Policies
- 9 Role Assignment
- 10 WLAN Configured

Specify whether WLAN is for Internal network or guest use for aruba-guest-network in Group default

Guest WLANs allow guests to access the Internet, while blocking access to the internal network. Guest WLANs are not encrypted, and at least require Web-based authentication. Internal WLANs typically employ encryption and strong 802.1X authentication. [More...](#)

Is this WLAN intended for internal use or for use by guests?

☐ Internal

☒ Guest

Back Next Cancel

CHOOSE THE AUTHENTICATION

The screenshot shows the Aruba Mobility Controller configuration page for a guest network. The left sidebar contains a navigation menu with 10 items: 1 WLAN, 2 Forwarding Mode, 3 Radio & VLAN, 4 Internal/Guest, 5 Authentication and Encryption, 6 Captive Portal, 7 Authentication Server, 8 Roles & Policies, 9 Role Assignment, and 10 WLAN Configured. The main content area is titled 'Specify Authentication and Encryption for aruba-guest-network in Group default'. It includes a slider to choose the level of security, ranging from 'More Secure' to 'Less Secure'. The options are:

- Captive portal with authentication via credentials(username and password) provided by user.
- Captive Portal with email registration.User's email is required but not verified
- Captive Portal with no authentication or registration
- Direct access to Internet (no Captive Portal)

At the bottom of the main content area are three buttons: 'Back', 'Next', and 'Cancel'. A red callout box with the text '1. Choose "with authentication"' points to the first option. Another red callout box with the text '2. Click Next' points to the 'Next' button.

DON'T CHOOSE ANY CAPTIVE PORTAL OPTIONS

The screenshot shows the Aruba Mobility Controller configuration page for Wireless LANs. The left sidebar contains a navigation menu with 10 items: Workflow, Help, WLAN, Forwarding Mode, Radio & VLAN, Internal/Guest, Authentication and Encryption, Captive Portal, Authentication Server, Roles & Policies, Role Assignment, and WLAN Configured. The main content area is titled 'Specify Captive Portal Options for aruba-guest-network in Group default'. It includes a checkbox for 'Enable Captive Portal' which is checked. Below this are fields for 'Template' (set to 'Custom HTML'), 'Page Design' (with tabs for 'Welcome Text' and 'Policy Text'), 'Background' (set to 'Default Image'), and 'Logo' (with a 'Choose File' button and 'no file selected' text). A 'Refresh >>' button is also present. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons. A red arrow points from the 'Next' button to a red speech bubble containing the text '1. Click Next'.

ARUBA networks MOILITY CONTROLLER | Aruba620

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

Configure WLAN/LANs

1 Group **2 Wireless LANs**

Workflow ? Help

1 WLAN
APGroup: default
SSID: aruba-guest-network

2 Forwarding Mode
Tunnel

3 Radio & VLAN
Radio Type: all
VLAN: 1

4 Internal/Guest
Guest

5 Authentication and Encryption
Guest

6 Captive Portal

7 Authentication Server

8 Roles & Policies

9 Role Assignment

10 WLAN Configured

Specify Captive Portal Options for aruba-guest-network in Group default

Captive portal provides web-based authentication. If captive portal is enabled, users who connect to this WLAN must authenticate by opening a web browser. They will be automatically redirected to the captive portal page and required to provide a username and password. Usernames and passwords can be stored either in a local database or on an external RADIUS server. [More...](#)

☒ Enable Captive Portal

Template Custom HTML

Page Design Welcome Text Policy Text

Background: Default Image

Logo: Choose File no file selected

Refresh >>

[Preview current settings](#)

Back Next Cancel

1. Click Next

ADD IDENTITY MANAGER AS AN AUTHENTICATION SERVER

1. Specify new server

2. Enter the details of your IDM

3. Shared secret key should match what you enter on IDM later

4. Click Ok

5. Click Next

ALLOW THE PRE-AUTHENTICATION TRAFFIC TO IDM

1. Select the aruba-guest-network-guest role

2. Select logon-control

3. Specify destination as IDM

4. Specify service as svc-https

5. Click Next

Roles/Policies/Rules	Policy Details	Role VLANs
guest	logon-control	
aruba-guest-network-guest	captiveportal	

Source	Dest	Service	Action
user	any	udp 68	deny
any	any	svc-icmp	permit
any	any	svc-dns	permit
any	any	svc-dhcp	permit
any	any	svc-pat	permit
any	host ...	svc-https	permit

Host IP: 192.168.1.27

Service: svc-https (tcp 443)

Back Next Cancel

SET THE ROLES

ARUBA networks MOILITY CONTROLLER | Aruba620

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Plan | Save Configuration

Configure WLAN/LANs

1 Group | **2 Wireless LANs**

1 WLAN
APGroup: default
SSID: aruba-guest-network

2 Forwarding Mode
Tunnel

3 Radio & VLAN
Radio Type: all
VLAN: 1

4 Internal/Guest
Guest

5 Authentication and Encryption
Guest

6 Captive Portal
Enabled

7 Authentication Server
N/A

8 Roles & Policies
2 Roles, 0 Policies

9 Role Assignment

10 WLAN Configured

Configure Role Assignment for aruba-guest-network in Group

After being authenticated, each client is assigned a role, which determines the resources to which the client will have access. You can assign the same role to all clients, or assign server-derived roles based on attributes returned by the authentication server at authentication time. [More...](#)

Pre-authentication role:

Authenticated role:

Back Next Cancel

1. Set the Roles

2. Click Next

FINISH THE WIZARD

The image displays two sequential screenshots of the Aruba Mobility Controller web interface, illustrating the final steps of the WLAN configuration wizard.

Top Screenshot: The 'WLAN Configuration is Complete' screen. The left sidebar shows the configuration steps: 1. Group, 2. Wireless LANs, 3. Radio & VLAN, 4. Internal/Guest, 5. Authentication and Encryption, 6. Captive Portal, 7. Authentication Server, 8. Roles & Policies, 9. Role Assignment, and 10. WLAN Configured. The main content area states: 'WLAN Configuration is Complete. Configuration of the WLAN aruba-guest-network is complete. More...'. It includes links: 'If you wish to configure another WLAN, click here.' and 'To repeat Wizard for another Group, click again.'. At the bottom, there are 'Back', 'Finish', and 'Cancel' buttons. A red callout bubble with the text '1. Click Finish' points to the 'Finish' button.

Bottom Screenshot: The 'Wireless LANs' summary screen. The left sidebar shows the configuration steps: 1. Group, 2. Wireless LANs, 3. Radio & VLAN, 4. Internal/Guest, 5. Authentication and Encryption, 6. Captive Portal, 7. Authentication Server, 8. Roles & Policies, 9. Role Assignment, and 10. WLAN Configured. The main content area shows the details for 'WLAN 1 (Created)': 'WLAN', 'APGroup: default', 'SSID: aruba-guest-network', and 'Forwarding Mode'. At the bottom, there are 'Back', 'Finish', and 'Cancel' buttons. A red callout bubble with the text '2. Click Finish' points to the 'Finish' button.

REDIRECT TO THE IDM PORTAL

1. Configuration > SECURITY > Authentication > L3 Authentication

2. Select Aruba-guest-network-cp_prof

3. Guest Login

4. User Login

5. Switch IP

6. Enter `https://{IDM-Name}/portal/{Controller-IP}/`

7. Enter `https://{IDM-Name}/portal/{Controller-IP}/success`

Captive Portal Authentication Profile > aruba-guest-network-cp_prof			
Default Role	guest	Default Guest Role	guest
Redirect Pause	0 sec	User Login	<input checked="" type="checkbox"/>
Guest Login	<input checked="" type="checkbox"/>	Logout popup window	<input type="checkbox"/>
Use HTTP for authentication	<input type="checkbox"/>	Minimum	5
Logon wait maximum wait	10	Threshold	60
Show FQDN	<input type="checkbox"/>	Non-	<input type="checkbox"/>
Login page	https://192.168.1.27/po	Welcome page	https://192.168.1.27/po
Show Welcome Page	<input checked="" type="checkbox"/>	Add switch IP address in URI	<input checked="" type="checkbox"/>
Allow only one active user session	<input type="checkbox"/>	Add	
Black List		Show the policy	<input type="checkbox"/>

ADD THE CONTROLLER TO IDM

The screenshot shows the 'RADIUS Clients' configuration window. It contains the following fields and callouts:

- Client:** A tab at the top left.
- Name:** A text field containing 'Aruba-600'. Callout 1: '1. Enter a name (used for description only)'.
- Device IP Address / Prefix Length:** A text field containing '10.10.20.2/32'. Callout 2: '2. Enter the IP address of the controller'. Below the field is the text: 'For example 192.168.1.1/32 or fec0:0001/128'.
- Secret:** A text field with masked characters '.....'. Callout 3: '3. Enter the same shared secret used on the Aruba RADIUS setup'.
- Confirm:** A text field with masked characters '.....'.
- Type:** A dropdown menu with 'Aruba' selected. Callout 4: '4. Specify Aruba for the Type'. Below the dropdown is the text: 'If your RADIUS client vendor is not listed, select Generic RADIUS Device'.
- Description:** A large empty text area.
- Port:** A text field containing '3799'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.



Thank you